BayRS Version 14.10

Part No. 308663-14.10 Rev 01
February 2000

4401 Great America Parkway
Santa Clara, CA 95054

Release Notes for BayRS Version 14.10 for the Passport 5430 and Passport 2430

NORTEL NETWORKS™

Copyright © 2000 Nortel Networks

All rights reserved. Printed in the USA. February 2000.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Bay Networks, ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FRE, LN, Optivity, Optivity Policy Services, PPX, and Quick2Config are registered trademarks, and Advanced Remote Node, ANH, ARN, ASN, BayRS, BaySecure, BayStack, BayStream, BCC, BCNX, BLNX, Centillion, EtherSpeed, FN, IP AutoLearn, Passport, SN, SPEX, Switch Node, System 5000, and TokenSpeed are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF

THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Nortel Networks NA Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN

IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Hard-Copy Technical Manuals ix
How to Get Help x

Release Notes for BayRS Version 14.10 for the Passport 2430 and Passport 5430

Hardware Platforms Supported 1
New Features 2
CES Supported Over ATM 2
Shaping Traffic Over an ATM PVC 2
Time Division Multiplexing (TDM) Services 3
General Guidelines 3
APPN on Passport 2430 Requires 32 MB of DRAM 3
Using Both Site Manager and the BCC 3
LED Sequence During Booting of Passport 5430 3
Traffic Filters Guidelines 4
Downloading Internet Routes from an ISP 5
Cisco Compatibility Issues Using PIM 5
Fragment Tagging in Bootstrap Messages 5
Cisco Drops RP Advertisement Messages with Zero Prefix Count 5
Routers Ignore RP Priority and Hash Value During RP Selection 6
ATM Half Bridge Guidelines 6
Managing BayRS 14.10 and Carrier Network Services (CNS) 1.2.0.0 6
OSPF Guidelines 7
IPsec Guidelines 7
IPsec 3DES Performance Considerations 7
IPsec Executable 8
Adding the IPsec File to the BayRS 14.10 Base Kernel 9

BayRS Bandwidth Broker for Differentiated Services 9
Event Database 10
Year 2000 Compliance 10
Using Embedded Web Server to Transfer Files 10
Configuring PU 4 and SDLC Link Stations 10
Configuring CES 11
Creating Multiple GRE Tunnels 12
Configuring NAT Dynamically 12
Protocol Prioritization No Call Filters and TCP Applications 12
Adding SDLC Changes Serial Parameter Settings 13
Configuring RADIUS Servers 14
BCC Guidelines 15
BCC and BayRS Compatibility 15
Deleting Interfaces with the BCC 15
Sending BCC Feedback 15
Memory Requirements 15
Interfaces Supported 16
Protocols Supported 16
Identifying Board Types 17
Operating Limitations and Cautions 20
Unsupported Features 20
Deleting ATM from a Router if Signaling Is Enabled 21
Signal Ports Settings on a Switch and Router Conflict 21
Creating FTP from the BCC 21
Using DVMRP with Interfaces with More than One IP Address 21
Deleting a Hybrid Mode Permanent Virtual Circuit (PVC) 21
Using DLSw/APPN Boundary Port with AS400s and Other Adjacent Link Stations . 21
Virtual Channel Connections (VCCs) Becoming Inactive 22
Accessing the Embedded Web Server Using Microsoft Internet Explorer 22
Router Loses IP Connection When Security Enabled 22
Protocols Supported 23
Standards Supported 26
Flash Memory Cards Supported 31

Tables

Table 1. Minimum PCR and SCR Settings for CES PVCs 11
Table 2. Default Settings for Serial Parameters without SDLC 13
Table 3. Default Settings for Serial Parameters with SDLC 13
Table 4. BCC Board Types: Passport 2430 18
Table 5. BCC Board Types: Passport 5430 19
Table 6. Standards Supported by Version 14.10 26
Table 7. Approved Flash Memory Cards 31

Preface

The Nortel Networks™ BayRS™ Version 14.10 is a software release that includes bug fixes and new features added since BayRS Version 14.00. These release notes contain guidelines for using BayRS Version 14.10 for the Passport 2430 and Passport 5430.

Hard-Copy Technical Manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the product for which you need documentation, then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase selected documentation sets, CDs, and technical publications through the collateral catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone Number
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Release Notes for BayRS Version 14.10 for the Passport 2430 and Passport 5430

This document contains the latest information about Nortel Networks BayRS Version 14.10, including information on the following topics:

Topic	Page
Hardware Platforms Supported	1
New Features	2
General Guidelines	3
BCC Guidelines	15
Operating Limitations and Cautions	20
Protocols Supported	23
Standards Supported	26
Flash Memory Cards Supported	31

Hardware Platforms Supported

The Passport 2430 and Passport 5430 router platforms are the only hardware platforms that support BayRS Version 14.10.

The Passport 2430 is a low-end multiservice access switch that provides a LAN connection and two slots for WAN adapter modules. The Passport 2430 supports a broad array of primary and backup connectivity options.

The Passport 5430 Multiservice Access Switch provides high-speed WAN connectivity to support the remote branch office.

New Features

The following sections provide brief descriptions of the new features in BayRS Version 14.10.

CES Supported over ATM

With BayRS 14.10, you can use Circuit Emulation Service (CES) over ATM for the Passport 5430. CES includes a set of services that support the emulation of existing time division multiplexing (TDM) circuits over an ATM network. For information about configuring CES services, refer to *Configuring ATM Services*. For information about configuring TDM services, refer to *Configuring TDM Services*.

Shaping Traffic over an ATM PVC

With BayRS 14.10 on the Passport 5430, you can shape traffic over an ATM PVC by configuring the following parameters:

- Service category
- AAL type
- VBR type
- Congestion indication
- Cell loss priority
- Initial and minimum cell rates
- Cell rate increase and decrease factors

For more information about how to configure these parameters to refine traffic across a PVC, see *Configuring ATM Services*.

Time Division Multiplexing (TDM) Services

With BayRS 14.10 on a Passport 5430, you can configure a time division multiplexing (TDM) circuit and transfer TDM data across an ATM WAN using circuit emulation services (CES). TDM provides a way to merge data from several sources into a single channel. TDM enables you to divide each channel into time slots and assign to each transmitting device at least one of the time slots for its transmission. For information about how to configure CES, refer to *Configuring ATM Services*.

General Guidelines

The following guidelines supplement the instructions in the BayRS Version 14.10 documentation set.

APPN on Passport 2430 Requires 32 MB of DRAM

To run Advanced Peer-to-Peer Networking (APPN) on the Passport 2430, you must purchase and install the 16 MB memory upgrade, for a total of 32 MB of dynamic RAM (DRAM).

Using Both Site Manager and the BCC

You can use either Site Manager or the BCC to manage Nortel Networks routers. If you want to use both tools, follow these guidelines:

- Do not try to use both Site Manager and the BCC to manage a single router during the same configuration session. You are prohibited from doing so with a lock-out mechanism.
- Site Manager cannot understand traffic filters you configured using the BCC.

LED Sequence During Booting of Passport 5430

During the boot sequence for the Passport 5430, the Boot LED remains on (green) and the Run LED lights green, indicating that the Passport 5430 is operational. Whenever the Boot LED is on (green), the Passport 5430 is in either Boot or Run mode. The description of the Boot sequence LEDs in *Installing and Operating the Passport 5430 Multiservice Access Switch* is incorrect.

Traffic Filters Guidelines

Follow these guidelines when configuring traffic filters:

- If you apply a traffic filter to a *multinetted interface* (that is, an interface with more than one IP address), the traffic filter might not work correctly. To ensure that the filter works correctly, you must assign the same filter to all of the IP addresses on the interface.
- Site Manager cannot understand traffic filters you have configured using the BCC.
- When you implement outbound traffic filters for LAN protocols, in some configurations the filters might cause a decline in throughput performance. For LAN circuits where the forwarding rate of the router is critical, monitor the throughput performance after configuring outbound traffic filters. If you notice an unacceptable performance degradation, try using inbound traffic filters.
- If you use Site Manager or the BCC to configure IP traffic filters with precedence values that are higher than the number of traffic filters configured, you might reach the maximum precedence value before you create the maximum number of filters. When you reach the maximum precedence value of 31 traffic filters, the router generates an error if you try to configure a filter with a precedence of 32. The system does not place you in extended filtering mode.

  For example, if you create the following five traffic filters, an error occurs when you create the fifth filter:

  Filter 1 precedence = 28

  Filter 2 precedence = 29

  Filter 3 precedence = 30

  Filter 4 precedence = 31

  Filter 5 precedence = 32 (error occurs here)

  As a workaround, you can take one of the following actions:

  -- Reassign the precedence value of traffic filters 1 through 5 to lower values.

  -- Use the Technician Interface to turn on extended filtering mode and let the system assign precedence values to additional traffic filters on the IP interface.

Downloading Internet Routes from an ISP

To minimize the time required to download routes from an Internet Service Provider (ISP), adjust two IP global parameters. Use the BCC to set the routing-table-indexes value to 10000 and the routing-table-deviation value to 50, as follows:

```
ip#routing-table-indexes 10000
ip#routing-table-deviation 50
```

See *Configuring IP, ARP, RIP, and OSPF Services* for more information about these commands.

Cisco Compatibility Issues Using PIM

This section describes Cisco compatibility issues that exist when running Protocol Independent Multicast (PIM) in a network that consists of both Cisco and Nortel Networks routers.

Fragment Tagging in Bootstrap Messages

In a PIM network in which Nortel Networks and Cisco routers interoperate, a Cisco router sends bootstrap packets that contain a fragment tag set to a zero value. When the Nortel Networks router receives these packets, it treats them as duplicate packets and immediately drops them.

To enable a Nortel Networks router to accept bootstrap packets from a Cisco router, set the Cisco Compatible parameter to Enable using Site Manager.

Cisco Drops RP Advertisement Messages with Zero Prefix Count

If you configure a Cisco router to serve as the bootstrap router (BSR) and you configure a Nortel Networks router to serve as an RP router for a PIM domain, the Cisco router drops any RP advertisement packet it receives from the RP router that contains a zero group prefix count. As a result, the Cisco router cannot advertise RP set information to all PIM routers in the domain.

To ensure that the Cisco router sends advertisement messages to all multicast group ranges using address 224.0.0.0/4, set the Cisco Compatible parameter to Enable.

Routers Ignore RP Priority and Hash Value During RP Selection

You configure multiple RPs responsible for the same or overlapping group ranges in a PIM domain. For RPs responsible for the same group ranges, a Cisco router selects the first RP on the RP list, regardless of the RP priority and hash value. For RPs responsible for overlapping group ranges, a Cisco router selects the router with the most specific group range, regardless of the RP priority and hash value.

As a workaround, configure only one RP router for each unique group range. This allows the Nortel Networks router and the Cisco router to select the same RP.

ATM Half Bridge Guidelines

BayRS Version 14.10 includes support of the ATM Half Bridge (AHB) feature.

Please be aware that some users, operating under certain conditions, may encounter issues such as the following:

- When AHB caches an unsecure host that it learned via ARP, the associated idle time is 0. The idle time remains at 0 and does not age correctly.
- When you reset the AHB, it stops forwarding traffic out of the AHB port.
- If you configure AHB on an ATM null PVC, the router may crash.

Managing BayRS 14.10 and Carrier Network Services (CNS) 1.2.0.0

The MIBs for BayRS 14.10 and Carrier Network Services (CNS) 1.2.0.0 share common structures, but have not been synchronized. This could cause object conflicts in network management applications managing networks that include both BayRS and CNS elements. If you want to manage both BayRS 14.10 and CNS 1.2.0.0 elements in your network, we recommend loading the MIB for each system into a separate instance of the network management application.

OSPF Guidelines

If you are using Open Shortest Path First (OSPF) services, please be aware of the following guidelines:

- As of BayRS Version 14.00, we do not support the OSPF backup soloist feature.
- According to RFC 2328, the cost of an OSPF route to an aggregated group of networks should be the distance to the furthest network in the group. A new MIB parameter, wfOspfAggrUseMaxCost, allows you to determine how to summarize the subnets using the area range. To use the furthest cost in the routing table, set this MIB parameter to **1** (Enable). If you accept the default, **2** (Disable), the OSPF route cost is represented as the shortest path to a network within the aggregated group of networks.

IPsec Guidelines

This section describes guidelines you should follow if you are using Internet Protocol Security (IPsec) services.

IPsec 3DES Performance Considerations

IPsec performance can vary greatly, and IPsec can impact router performance in general. Factors that affect performance are the cryptographic algorithms that IPsec uses, which consume substantial CPU resources, other protocols and features running on the slot that share the same CPU resources as IPsec, and the processing power of the BayRS router.

The following information will help you plan and manage CPU resources in BayRS routers configured with IPsec.

Greater security can adversely affect performance. Before deploying IPsec, identify the data traffic that must be protected. Effective traffic analysis might result in minimal performance impact on the router. Configure IPsec to bypass traffic that does not need to be protected, thereby reducing the CPU resources used. Also, the amount of CPU resources required varies significantly for different encryption and authentication algorithms.

These algorithms are listed in order of increasing CPU consumption and security:

- MD5
- SHA1
- DES
- DES with MD5
- DES with SHA1
- 3DES
- 3DES with MD5
- 3DES with SHA1

In addition, the key generation and periodic rekeying done by IKE Diffie Hellman imposes a CPU burden. Therefore, consider the keying intervals for IKE and for IPsec that you choose during configuration. Less frequent rekeying reduces the burden on the CPU. Consider rekeying the Phase 1 (IKE) SAs less frequently than the IPsec SAs.

Finally, the packet size influences the performance of the router. Smaller packet sizes at a given data rate impose a greater processing load than larger packet sizes.

You can optimize performance by using the information in this section to plan and manage CPU resources. For example, BayRS IPsec on a BN can fill a 2 Mb/s WAN pipe with bidirectional DES-encrypted traffic. Conversely, 3DES + SHA1 traffic with aggressive Phase 1 (IKE) and IPsec rekeying (for example, every 10 minutes) might cause significant performance degradation under heavy traffic loads.

You might experience SNMP timeouts during periods when the router is carrying peak loads of protected traffic.

IPsec Executable

To use the IPsec option, you must purchase a separate IPsec CD that contains either the 56-bit (DES) or both triple DES (3DES) and the DES cryptographic API executable (*capi.ppc*) for the BayRS software. Purchase the CD for the router software version you are running. Follow the instructions included with the CD or in *Configuring IPsec Services* to install the IPsec option.

Adding the IPsec File to the BayRS 14.10 Base Kernel

To use IPsec, you must use Image Builder to add an IPsec file to the BayRS 14.10 base kernel. The IPsec file is located on a separate CD. To install IPsec, follow the instructions included on the IPsec CD. You do not have to modify or add anything to Site Manager.

BayRS Bandwidth Broker for Differentiated Services

To implement a differentiated services network using a BayRS bandwidth broker, you must install the BayRS Bandwidth Broker, also known as the *policy server*, software on a PC running Windows NT® 4.0. The Nortel Networks router that communicates with the bandwidth broker must be operating with BayRS Version 13.20 or later software.

To download the policy server software and learn how to configure it:

1. **Go to the Router Management Labs page at *http://www.nortelnetworks.com/rml*.**
2. **Click on Software Solutions.**
3. **If you are a registered user, enter your email address. If not, register.**

   You see a list of solutions for which you can download software.
4. **Scroll through the list to locate the Policy Server.**

   From here you can download the software and the user manual.

Installation Script for the Passport 5430

The installation script for the Passport 5430 is *inst_pp5430.bat*. References to a script named *inst_pp5400.bat* in Appendix B of *Installing and Operating the Passport 5430 Multiservice Access Switch* are incorrect.

Event Database

You can view the event database on the World Wide Web and the BayRS Online Library Version 14.10 CD. To access the event database on the World Wide Web, go to: *http://support.baynetworks.com/library/tpubs/events*

To access the event database on the BayRS Online Library Version 14.10 CD, follow the instructions in the CD booklet.

The event database includes a search facility that allows you to sort events by entity number, event number, severity, and text of the event message. For example, you can list only the warning messages for the IPX entity.

Year 2000 Compliance

BayRS Version 14.10 is Year 2000 Compliance Certified by Nortel Networks. The software has successfully passed the Nortel Networks Test Procedure, which tests conformance to the Nortel Networks Year 2000 compliance definition. For more information, see the Nortel Networks Year 2000 Web Site at *http://www.nortelnetworks.com/corporate/year2000/bay/*.

Using Embedded Web Server to Transfer Files

When you use the embedded Web server to transfer files to or from the router, HTTP (Hypertext Transfer Protocol) encapsulates the data. You do not need to be concerned with selecting a file format (text or binary, for example) the way you would if you were using FTP (File Transfer Protocol) or TFTP (Trivial File Transfer Protocol) to transfer the files.

For example, to transfer an image file to the router, use your browser's default file format type to transfer the file to the router's FLASH memory. The file arrives at the router as an image file from which you can boot the router.

Configuring PU 4 and SDLC Link Stations

If you use PU 4 devices with Synchronous Data Link Control (SDLC) and modulo 128, set the SDLC parameters MAXOUT and MAXIN to 127. You see these parameters in the SDLC Link Station Configuration window. For instructions on setting these parameters, see *Configuring SDLC Services*.

Configuring CES

To correctly support CBR (constant bit rate) bandwidth for CES, PVCs that are external to the Passport 5430 must provide a minimum PCR (peak cell rate) and SCR (sustained cell rate). If the PVCs do not provide these minimum rates, the PVCs will experience data underruns, and the CES circuit will lose data.

The BCC and Site Manager automatically compute and set the PCR and SCR rates on the Passport 5430 when you specify the timeslot and timeslot-subrate values in the BCC or the Number of Timeslots and Per Timeslot Subrate values in Site Manager. Table 1 lists the minimum PCR and SCR settings required for the PVCs on the switch(es) in the ATM network, in order for the PVCs to carry CES traffic between Passport 5430 routers.

Table 1. Minimum PCR and SCR Settings for CES PVCs

Timeslots	Subrate (Kb/sec)	Data Rate (Kb/sec)	PCR (cells/sec)	SCR (cells/sec)
1	56	56	187	187
1	64	64	215	215
2	64	128	427	427
3	64	192	640	640
4	64	256	852	852
5	64	320	1066	1066
6	64	384	1278	1278
7	64	448	1491	1491
8	64	512	1703	1703
9	64	576	1916	1916
10	64	640	2130	2130
11	64	704	2342	2342
12	64	768	2555	2555
13	64	832	2767	2767
14	64	896	2980	2980
15	64	960	3193	3193
16	64	1024	3406	3406
17	64	1088	3618	3618
18	64	1152	3622	3622

Creating Multiple GRE Tunnels

When creating multiple GRE tunnels dynamically, you can configure a maximum of five point-to-point GRE tunnels. In multipoint configurations, you can configure 64 GRE tunnels per interface.

Configuring NAT Dynamically

When you configure a local or global interface for NAT in dynamic mode, the router returns an SNMP set error. However, this error does not affect the configuration of the router.

Protocol Prioritization No Call Filters and TCP Applications

Using a no call filter that applies to any TCP application can cause TCP to retransmit the filtered packet.

When two routers running a TCP application are connected using a demand line, and the demand line becomes inactive, the TCP application remains connected.

If a demand line configured with a no-call filter goes down, the no-call filter drops the TCP packet that matches the no-call filter rule. Because TCP never receives an acknowledgment that the packet was dropped, the TCP application continues to retransmit that packet until the connection times out and the application stops operating.

Note: No-call filters are specific to dial services. For additional information about traffic filters and protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization*.

Adding SDLC Changes Serial Parameter Settings

When you configure SDLC on a serial interface, the router software automatically changes the values for the following serial parameters:

- cable type
- clock source
- internal clock speed
- signal mode

Defaults for serial parameters, without SDLC, are listed in Table 2.

Table 2. Default Settings for Serial Parameters without SDLC

Parameter	Default Setting
cable type	null
clock source	external
internal clock speed	clk64k
signal mode	balanced

After you add SDLC to an interface, the settings for the serial parameters change. The new settings are listed in Table 3.

Table 3. Default Settings for Serial Parameters with SDLC

Parameter	Default Setting
cable type	rs232
clock source	internal
internal clock speed	clk19200
signal mode	unbalanced

Configuring RADIUS Servers

To enable RADIUS authentication for multilevel access or to use vendor-specific attributes (VSAs), you must configure the BSAC RADIUS server with the following files:

- *bayrs.dct*
- *vendor.ini*
- *dictiona.dcm*

These files load at server startup and enable the server to recognize the vendor-specific RADIUS clients. You can locate these files in the *bsac* directory on the BayRS Router and Site Manager Software update CD.

- To configure a Nortel Networks RADIUS server, copy the three files to the directory that you define at installation time (typically *C:\RADIUS\Service*).
- To configure a non-Nortel Networks RADIUS server, use the *bayrs.dct* file as a reference to change the existing RADIUS dictionary. Because *bayrs.dct* is in the format of some popular RADIUS servers, you might be able to use it as a direct replacement for the existing RADIUS dictionary. For more information, see the vendor's documentation.

Note: To use RADIUS with IP utilities such as FTP, NTP, HTTP, and Telnet, your RADIUS server must support VSAs.

The RADIUS dictionary file (*bayrs.dct*) defines the Nortel Networks vendor-specific attributes. The Nortel Networks vendor ID is 1584, as allocated by the Internet Assigned Numbers Authority. Use this ID in the header when using VSAs.

For more information on	See this document
RADIUS	*Configuring RADIUS*
BaySecure Access Control	*BaySecure Access Control Administration Guide* (for your specific platform: UNIX, Netware, or Windows NT)
Multilevel Access	*Using the Bay Command Console (BCC™)*

BCC Guidelines

The BCC is a command-line interface for configuring Nortel Networks devices.

Before using the BCC, see the following guidelines for using the software and the platforms, protocols, interfaces, and hardware modules that the BCC supports.

BCC and BayRS Compatibility

Starting with BayRS Version 14.00, the BCC software version number matches that of BayRS. For example, the version of BCC that ships with BayRS Version 14.10 is BCC Version 14.10. We have made this change to help you align versions of BCC with versions of BayRS.

Deleting Interfaces with the BCC

Before using the BCC to delete an interface, make sure that you did not use Site Manager to configure the interface with a protocol that the BCC does not recognize. If you did, use Site Manager to delete the interface.

Sending BCC Feedback

After you use the BCC, we welcome your feedback. Please visit the BCC Web site at the following URL, where you can leave a message:

http://support.baynetworks.com/library/tpubs/bccfeedbk

Memory Requirements

To use the BCC, each slot on the router must have:

- 16 MB of dynamic RAM (DRAM)
- 2 MB of free memory available when you start the BCC

If you try to start the BCC with insufficient DRAM or free memory on a slot, the BCC returns the following message. In this case, you must use Site Manager instead of the BCC to configure the router.

```
**Error** Unable to load bcc command from file system.
Loadable Module: bcc.exe
```

Interfaces Supported

You can use BCC commands to configure the following interfaces:

- ATM (ATM DXI only on the Passport 2430)
- Console
- DSU/CSU
- Ethernet
- FDDI (Passport 5430 only)
- FE1
- FT1
- ISDN/BRI
- MCE1/MCT1 (Passport 5430 only)
- Serial (synchronous)
- Virtual (referred to in Site Manager as Circuitless IP)
- V.34 Modem

Protocols Supported

You can use BCC commands to configure the following protocols and services:

- Access (multiuser access accounts)
- ARP
- ATM (ATM DXI only on the Passport 2430)
- BGP (including accept and announce policies)
- Dial backup
- Dial-on-demand
- DLSw
- DNS
- DVMRP (including accept and announce policies)
- Frame relay (multilink not supported)
- FTP
- GRE
- HTTP
- IGMP

- IP (including accept policies, adjacent hosts, static routes, and inbound traffic filters)
- IPX (including static-netbios-route)
- IPXWAN
- LLC2
- MPOA (Passport 5430 only)
- NAT
- NHRP
- NTP
- OSPF (including accept and announce policies)
- PPP (certain line parameters only; no multiline or multilink supported)
- Proprietary Standard Point-to-Point
- RADIUS
- RIP (including accept and announce policies)
- Router discovery (RDISC)
- SDLC
- SNMP
- Source route bridge
- Spanning tree
- Syslog
- Telnet
- TFTP
- Transparent Bridge
- VRRP (Virtual Router Redundancy Protocol)

Identifying Board Types

Table 4 and Table 5 identify the Board Type parameter values displayed by the BCC. Use the “BCC Board Type” column to find a hardware module in a Passport 2430 or Passport 5430 router configuration.

Table 4 lists the board types for the Passport 2430.

Table 4. BCC Board Types: Passport 2430

BCC Board Type	Technician Interface or MIB Module ID	Description
arnmbsfetx	8728	ARN 10/100BASE-TX Ethernet Module
arnssync	8736	ARN Serial Adapter Module
arnv34	8752	ARN V34 Modem Module
arndcsu	8768	56/64K DSU/CSU Module
arnisdns	8784	ARN ISDN BRI S/T Adapter Module
arnisdnu	8800	ARN ISDN BRI U Adapter Module
arnft1	8776	T1/FT1 DSU/CSU Adapter Module
arnfe1	8780	E1/FE1 DSU/CSU Adapter Module

Table 5 lists the board types for the Passport 5430.

Table 5. BCC Board Types: Passport 5430

BCC Board Type	Technician Interface or MIB Module ID	Description
arnssync	8736	ARN Serial Adapter Module
arnv34	8752	ARN V34 Modem Module
arnft1	8776	T1/FT1 DSU/CSU Adapter Module
arnfe1	8780	E1/FE1 DSU/CSU Adapter Module
arndcsu	8768	56/64K DSU/CSU Module *(not supported)*
arnisdns	8784	ARN ISDN BRI S/T Adapter Module
arnisdnu	8800	ARN ISDN BRI U Adapter Module
fbrmbfen	8000	FBR Ethernet Module

Operating Limitations and Cautions

Be aware of the following limitations when using BayRS 14.10.

Unsupported Features

BayRS 14.10 does not support the following features and capabilities:

- Firewall-1.
- DES-40 WAN Encryption Option (WEP) or DES-56 WAN Encryption Option (WEP) to perform PPP or frame relay layer 2 encryption. We recommend that you use Internet Protocol Security (IPsec) services for security.
- Hi/fn™ LZS® data compression.
- 802.1Q tagging for VLAN (virtual LAN) connections on the Passport 2430. (802.1Q tagging is available on the Passport 5430.)
- RMON.
- Mini-RMON on the Passport 2430. (Mini-RMON is available on the Passport 5430.)
- Virtual Router Redundancy Protocol (VRRP) over LAN Emulation (LANE) and Multi-Protocol Over ATM (MPOA) on the same service record.
- Failover and load Balancing for ATM VCs. You can configure multiple ATM virtual circuits (VCs) to the same destination address. However, this kind of configuration does not provide load balancing or failover support.
- The 56/64K DSU/CSU module type on the Passport 5430.
- The OSPF backup soloist feature.
- The following three MIB attributes: wfAtmizerVclRxOctets, wfAtmizerVclTxOctets, and wfAtmizerVclTxClipFrames. Ignore the values that these statistics return.
- The ATM traffic parameter maximum burst size (MBS) on the 5782 processor modules.
- Bandwidth on Demand on the Passport 2430. (Bandwidth on Demand is available on the Passport 5430.)
- X.25 PAD (packet assembler/disassembler).

Deleting ATM from a Router if Signaling Is Enabled

Do not delete ATM from a Passport 5430 if you enabled signaling on an ATM circuit. If you try to delete ATM in this situation, Site Manager, the BCC, or the Technician Interface restarts after a few minutes.

Signal Ports Settings on a Switch and Router Conflict

If you are using a switch with signal ports set to V3.1, be sure to set the signaling setting on the router to V3.1. If you accept the default setting of V3.0 for the router, the router faults repeatedly until you change the setting to V3.1.

Creating FTP from the BCC

From the BCC, if you create FTP on the router, then delete it and recreate it, the BCC faults. In this case, you must restart the BCC and create FTP on the router again.

Using DVMRP with Interfaces with More than One IP Address

You cannot use the BayRS Version 14.10 implementation of Distance Vector Multicast Routing Protocol (DVMRP) with circuits with multinetted interfaces (that is, interfaces with more than one IP address).

Deleting a Hybrid Mode Permanent Virtual Circuit (PVC)

If you configure source route bridging on a router, do not delete hybrid mode PVCs. If you do, all slots restart.

Using DLSw/APPN Boundary Port with AS400s and Other Adjacent Link Stations

Do not configure any explicit APPN adjacent link stations on the DLSw/APPN boundary (VCCT) port, unless you are certain that the adjacent link station (for example, an AS400) will not attempt to connect to the APPN node. Otherwise, the DLSw/APPN boundary (VCCT) function fails to operate correctly and the router might restart.

Virtual Channel Connections (VCCs) Becoming Inactive

On the 5782 MPE, BayRS 14.10 does not release virtual channel connections when they time out. To maintain the availability of VCCs for new activities, configure a LAN emulation client (LEC) other than the router to release the inactive VCCs.

Accessing the Embedded Web Server Using Microsoft Internet Explorer

When you access the embedded Web server using Microsoft® Internet Explorer Version 4.72.2106.8, the file page is blank. However, Internet Explorer Version 4.72.3110.8 works correctly. We suggest that you upgrade to Version 4.72.3110.8 or later.

Router Loses IP Connection When Security Enabled

If you change the setting of the router's IP Security feature (MIB variable wfIpIntfCfgEnableSecurity) from Disabled to Enabled, the router loses its IP connection. You must reboot the router.

Protocols Supported

BayRS Version 14.10 supports the following bridging/routing protocols and router configuration features:

- Advanced Peer-to-Peer Networking (APPN)
- AppleTalk and AppleTalk Update Routing Protocol (AURP)
- Asynchronous transfer mode (ATM) (on the Passport 5430 only)
- ATM Data Exchange Interface (ATM DXI)
- ATM Half Bridge (AHB)
- ATM LAN Emulation (802.3 and 802.5)
- Bandwidth Allocation Protocol (BAP)
- Binary Synchronous Communication Type 3 (BSC3)
- Bisync over TCP (BOT)
- Bootstrap Protocol (BootP)
- Border Gateway Protocol (BGP-3 and BGP-4)
- Classless interdomain routing (CIDR)
- Data compression (WCP)
- Data link switching (DLSw)
- DECnet Phase IV
- Differentiated services
- Distance Vector Multicast Routing Protocol (DVMRP)
- Dynamic Host Configuration Protocol (DHCP)
- Exterior Gateway Protocol-2 (EGP-2)
- File Transfer Protocol (FTP)
- Frame relay (PVC, SVC)
- HP Probe
- Hypertext Transfer Protocol (HTTP)
- Integrated Services Digital Network (ISDN)
- Interface redundancy (proprietary)

- Internet Control Message Protocol (ICMP)
- Internet Gateway Management Protocol (IGMP)
- Internet Key Exchange (IKE)
- Internet Packet Exchange (IPX)
- Internet Protocol (IP)
- Internet Stream Protocol (ST2)
- IP Security (IPsec)
- IPsec Encapsulating Security Payload (ESP)
- Layer 2 Tunneling Protocol (L2TP)
- Learning bridge
- Logical Link Control 2 (LLC2)
- Multicast OSPF (MOSPF)
- Multiprotocol Over ATM (MPOA)
- Native Mode LAN (NML)
- Network Time Protocol (NTP)
- Open Shortest Path First (OSPF)
- Open Systems Interconnection (OSI)
- Point-to-Point Protocol (PPP)
- Polled Asynch (PAS), also called Asynch Passthru over TCP
- Protocol prioritization
- Qualified Logical Link Control (QLLC)
- RaiseDTR dialup
- Remote Authentication Dial-In User Service (RADIUS)
- Resource Reservation Protocol (RSVP)
- Router discovery (RDISC)
- Router redundancy (proprietary)
- Routing Information Protocol (RIP)
- Service Advertisement Protocol (SAP)

- Simple Network Management Protocol (SNMP)
- Source route bridging (SRB)
- Source route bridging over ATM permanent virtual circuits (PVCs)
- Spanning tree
- Switched Multimegabit Data Service (SMDS)
- Synchronous Data Link Control (SDLC)
- Telnet (inbound and outbound)
- Transmission Control Protocol (TCP)
- Transparent bridge
- Transparent-to-source routing translation bridge
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)
- V.25bis dialup
- Virtual Network Systems (VINES)
- Virtual Router Redundancy Protocol (VRRP)
- X.25 with QLLC
- Xerox Network System (XNS)
- XMODEM and YMODEM

Standards Supported

Table 6 lists the Request For Comments (RFCs) and other standards documents with which Version 14.10 complies. BayRS Version 14.10 might support additional standards that are not listed in this table.

Table 6. Standards Supported by Version 14.10

Standard	Description
ANSI T1.107b-1991	Digital Hierarchy -- Supplement to formats specifications
ANSI T1.404	DS3 Metallic Interface Specification
ANSI X3t9.5	Fiber Distributed Data Interface (FDDI)
Bellcore FR-440	Transport Systems Generic Requirements (TSGR)
Bellcore TR-TSY-000009	Asynchronous Digital Multiplexes, Requirements, and Objectives
Bellcore TR-TSY-000010	Synchronous DS3 Add-Drop Multiplex (ADM 3/X) Requirements and Objectives
FIPS 46-2	Data Encryption Standard (DES)
FIPS 81	DES Modes of Operation (ECB, CBC)
IEEE 802.1	Logical Link Control (LLC)
IEEE 802.1Q	IEEE 802.1Q VLAN tagging
IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
IEEE 802.5	Token Ring Access Method and Physical Layer Specifications
IEEE 802.1D	Spanning Tree Bridges
ITU Q.921	ISDN Layer 2 Specification
ITU Q.931	ISDN Layer 3 Specification
ITU X.25	Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuits
RFC 768	User Datagram Protocol (UDP)
RFC 791	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)
RFC 813	Window and Acknowledgment Strategy in TCP

(continued)

Table 6. Standards Supported by Version 14.10 *(continued)*

Standard	Description
RFC 826	Ethernet Address Resolution Protocol
RFC 827	Exterior Gateway Protocol (EGP)
RFC 854	Telnet Protocol Specification
RFC 855	Telnet Option Specification
RFC 856	Telnet Binary Transmission
RFC 857	Telnet Echo Option
RFC 858	Telnet Suppress Go Ahead Option
RFC 859	Telnet Status Option
RFC 860	Telnet Timing Mark Option
RFC 861	Telnet Extended Options: List Option
RFC 863	Discard Protocol
RFC 877	Transmission of IP Datagrams over Public Data Networks
RFC 879	TCP Maximum Segment Size and Related Topics
RFC 888	"STUB" Exterior Gateway Protocol
RFC 894	Transmission of IP Datagrams over Ethernet Networks
RFC 896	Congestion Control in IP/TCP Internetworks
RFC 903	Reverse Address Resolution Protocol
RFC 904	Exterior Gateway Protocol Formal Specification
RFC 919	Broadcasting Internet Datagrams
RFC 922	Broadcasting Internet Datagrams in Subnets
RFC 925	Multi-LAN Address Resolution
RFC 950	Internet Standard Subnetting Procedure
RFC 951	Bootstrap Protocol
RFC 959	File Transfer Protocol
RFC 994	Protocol for Providing the Connectionless-Mode Network Service
RFC 1009	Requirements for Internet Gateways
RFC 1027	Using ARP to Implement Transparent Subnet Gateways
RFC 1042	Transmission of IP over IEEE/802 Networks
RFC 1058	Routing Information Protocol

(continued)

Table 6. Standards Supported by Version 14.10 *(continued)*

Standard	Description
RFC 1075	Distance Vector Multicast Routing Protocol (DVMRP)
RFC 1076	Redefinition of Managed Objects for IEEE 802.3 Repeater Devices (AN hubs only)
RFC 1079	Telnet Terminal Speed Option
RFC 1084	BOOTP Vendor Information Extensions
RFC 1091	Telnet Terminal-Type Option
RFC 1108	Security Options for the Internet Protocol
RFC 1112	Host Extensions for IP Multicasting Appendix I, Internet Group Management Protocol
RFC 1116	Telnet Line-Mode Option
RFC 1139	Echo Function for ISO 8473
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157	Simple Network Management Protocol (SNMP)
RFC 1163	BGP-2 (obsoleted by RFC 1267)
RFC 1164	Application of BGP in the Internet
RFC 1166	Internet Numbers
RFC 1188	Proposed Standard for the Transmission of IP over FDDI
RFC 1191	Path MTU Discovery
RFC 1209	Transmission of IP Datagrams over SMDS
RFC 1212	Concise MIB Definitions
RFC 1213	MIB for Network Management of TCP/IP-Based Internets
RFC 1267	Border Gateway Protocol 3 (BGP-3; obsoletes RFC 1163)
RFC 1293	Inverse ARP for Frame Relay (obsoleted by RFC 2390)
RFC 1294	Multiprotocol Interconnect over Frame Relay (obsoleted by RFC 1490 and RFC 2427)
RFC 1304	Definition of Managed Objects for the SIP Interface Type
RFC 1305	Network Time Protocol
RFC 1315	Management Information Base for Frame Relay DTEs (obsoleted by RFC 2115)
RFC 1321	MDS Digest Algorithm
RFC 1323	TCP Extensions for High Performance

(continued)

Table 6. Standards Supported by Version 14.10 *(continued)*

Standard	Description
RFC 1331	Point-to-Point Protocol (PPP; obsoleted by RFC 1661)
RFC 1332	PPP Internet Protocol Control Protocol (IPCP)
RFC 1333	PPP Link Quality Monitoring (obsoleted by RFC 1989)
RFC 1334	PPP Authentication Protocols
RFC 1350	The TFTP Protocol (Revision 2)
RFC 1356	Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode
RFC 1376	PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1377	OSI over PPP
RFC 1378	PPP AppleTalk Control Protocol (ATCP)
RFC 1390	Transmission of IP and ARP over FDDI Networks
RFC 1403	BGP OSPF Interaction
RFC 1434	Data Link Switching: Switch-to-Switch Protocol
RFC 1483	Multiprotocol Encapsulation over ATM AAL5
RFC 1490	Multiprotocol Interconnect over Frame Relay (obsoletes RFC 1294, obsoleted by RFC 2427)
RFC 1541	Dynamic Host Configuration Protocol
RFC 1552	The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC 1577	Classical IP and ARP over ATM
RFC 1585	MOSPF: Analysis and Experience
RFC 1634	Novell IPX over Various WAN Media (IPXWAN)
RFC 1638	PPP Bridging Control Protocol (BCP)
RFC 1654	Border Gateway Protocol 4 (BGP-4; obsoleted by RFC 1771)
RFC 1661	Point-to-Point Protocol (PPP; obsoletes RFC 1331)
RFC 1662	PPP in HDLC-like Framing
RFC 1717	PPP Multilink Protocol (MP; obsoleted by RFC 1990)
RFC 1755	Signaling Support for IP over ATM
RFC 1762	PPP Banyan VINES Control Protocol (BVCP)
RFC 1763	PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1764	PPP XNS IDP Control Protocol (XNSCP)
RFC 1771	Border Gateway Protocol 4 (BGP-4; obsoletes RFC 1654)

(continued)

Table 6. Standards Supported by Version 14.10 *(continued)*

Standard	Description
RFC 1795	Data Link Switching: Switch-to-Switch Protocol, Version 1
RFC 1819	Internet Stream Protocol, Version 2
RFC 1974	PPP Stac LZS Compression Protocol
RFC 1989	PPP Link Quality Monitoring (obsoletes RFC 1333)
RFC 1990	PPP Multilink Protocol (MP; obsoletes RFC 1717)
RFC 2068	HTTP Version 1.1
RFC 2069	An extension to HTTP: Digest Access Authentication
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 2115	Management Information Base for Frame Relay DTEs Using SMIv2 (obsoletes RFC 1315)
RFC 2138	Remote Authentication Dial-In User Service (RADIUS)
RFC 2139	RADIUS Accounting
RFC 2166	Data Link Switching, Version 2.0, Enhancements
RFC 2178	OSPF Version 2
RFC 2205	Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification
RFC 2338	Virtual Router Redundancy Protocol
RFC 2385	Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 2390	Inverse Address Resolution Protocol (obsoletes RFC 1293)
RFC 2403	Use of HMAC-MD5-96 within ESP and AH
RFC 2404	Use of HMAC-SHA-1-96 within ESP and AH
RFC 2405	ESP DES-CBC Cipher Algorithm with Explicit IV
RFC 2406	IP Encapsulating Security Payload (ESP)
RFC 2407	Internet IP Security Domain of Interpretation for ISAKMP
RFC 2409	Internet Key Exchange (IKE)
RFC 2410	NULL Encryption Algorithm and Its Use with IPsec
RFC 2427	Multiprotocol Interconnect over Frame Relay (obsoletes RFC 1294 and RFC 1490)
RFC 2451	ESP CBC-Mode Cipher Algorithms
VINES 4.11	BayRS works with the Banyan VINES 4.11 standard. BayRS Version 8.10 (and later) also supports VINES 5.50 sequenced routing.

Flash Memory Cards Supported

You use Personal Computer Memory Card International Association (PCMCIA) flash memory cards to store the software image and the configuration files in Nortel Networks routers. Software images for BayRS 14.10 require 8 or 16 MB flash cards; however, you can store configuration files on 4 MB flash cards.

Table 7 lists the flash memory cards approved for use.

Table 7. Approved Flash Memory Cards

Size	Vendor	Part Number
4 MB	Advanced Micro Devices (AMD)	AMC004CFLKA-150
	AMP	797262-3
		797263-2
	Centennial	FL04M-20-11119
		FL04M-20-11138
	Epson	HWB401BNX2
	IBM	IBM1700400D1DA-25
	Intel	IMC004FLSAQ1381
8 MB	AMD	AMC008CFLKA-150
		AMC008CFLKA-200
		AMC008CFLKA-250
		AMC008DFLKA-150
		AMC008DFLKA-200
		AMC008DFLKA-250
	Centennial	FL08M-25-11119-01
		FL08M-15-11119-01
		FL08M-20-11138
		FL08M-20-11119-01
	Epson	HWB801BNX0
	Intel	IMC008FLSP/Q1422
	Centennial (Strata-Flash)	FL08-20-11736-J5-61

(continued)

Table 7. Approved Flash Memory Cards *(continued)*

Size	Vendor	Part Number
16 MB	Epson	HWB161BNX2
	Centennial (Strata-Flash)	FL16-20-11736-J5-61
32 MB	Centennial	FL32M-20-11119-67